HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 1.1
CÀI ĐẶT HỆ ĐIỀU HÀNH MÁY TRẠM WINDOWS

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

Rèn luyện kỹ năng cài đặt và quản trị HĐH máy trạm Windows cho người dùng với các dịch vụ cơ bản

1.2 Phần mềm ảo hóa VMWare Workstation

VMware là một phần mềm ảo hóa, được sử dụng để tạo ra và quản lý các máy ảo (Virtual Machines – VMs). Với VMware, ta có thể chạy nhiều hệ điều hành khác nhau trên cùng một máy tính vật lý, cho phép tận dụng tài nguyên hiệu quả hơn.

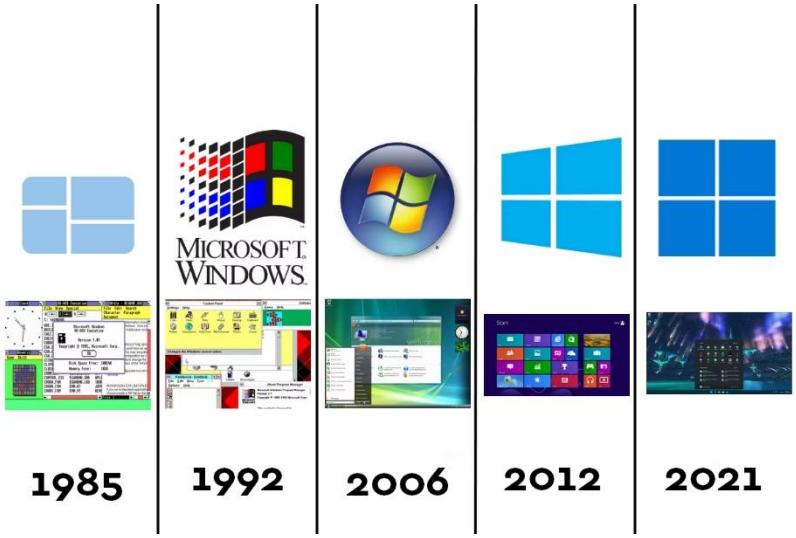
Các ứng dụng chính của VMware bao gồm:

- Ảo hóa máy chủ (Server Virtualization): Cho phép nhiều hệ điều hành hoặc máy chủ ảo chạy trên một máy chủ vật lý duy nhất.
- Phát triển và kiểm thử phần mềm: Giúp nhà phát triển chạy và kiểm tra các ứng dụng trên nhiều nền tảng mà không cần phần cứng riêng biệt.
- Triển khai và quản lý hệ thống: Các doanh nghiệp sử dụng để quản lý hạ tầng ảo hóa, triển khai hệ điều hành, ứng dụng và hệ thống mạng ảo.
- Chạy các hệ điều hành khác nhau song song: Người dùng có thể cài đặt và sử dụng nhiều hệ điều hành trên cùng một máy tính.

1.3 Hệ điều hành Windows

1.3.1 Lịch sử phát triển của Windows

Hệ điều hành Windows của Microsoft đã trải qua nhiều thăng trầm và đổi mới



Hình 1 – Các giai đoạn cơ bản của Windows

1.3.1.1 Giai đoạn đầu: Sự ra đời và những phiên bản Windows đầu tiên (1985 - 1995)

- Windows 1.0 (1985) được phát hành như một giao diện đồ họa chạy trên MS-DOS.

- Windows 2.x (1987 - 1990) cải thiện giao diện và tính năng.
- Windows 3.x (1990 - 1994) mang lại nhiều nâng cấp quan trọng, Windows 3.1 trở thành phiên bản thành công nhất.

1.3.1.2 Giai đoạn Windows 9x (1995 - 2001)

- Windows 95 (1995) ra mắt với giao diện hoàn toàn mới, giới thiệu nút "Start" và Taskbar.
- Windows 98 (1998) hỗ trợ Internet Explorer, tăng cường tính tương thích.
- Windows ME (2000) kém ổn định, nhưng đánh dấu cuối cùng của dòng Windows 9x.

1.3.1.3 Windows XP (2001 - 2006)

- Windows XP (2001) kết hợp hai dòng Windows 9x và Windows NT, giao diện đẹp, bảo mật cao, trở thành một trong những phiên bản thành công nhất

1.3.1.4 Windows 7 và Windows 8

- Windows 7 (2009) cải thiện tốc độ, tính ổn định, giao diện tối ưu hóa, trở thành một trong những phiên bản Windows được ưa chuộng nhất.
- Windows 8 (2012) thiết kế giao diện mới cho các thiết bị cảm ứng, nhưng bị chỉ trích do không thân thiện với người dùng.
- Windows 8.1 (2013) tăng cường tính năng tùy chỉnh, nhưng chưa đáp ứng được kỳ vọng của người dùng.

1.3.1.5 Windows 10 và Windows 11

- Windows 10 (2015) kết hợp tính năng tốt nhất từ Windows 7 và Windows 8, nhận được đánh giá cao về sự linh hoạt và hiệu năng.
- Windows 11 (2021) ra mắt với giao diện mới, hỗ trợ chạy ứng dụng Android, được kỳ vọng sẽ tiếp tục đẩy mạnh sự phát triển của Windows.

1.3.2 Kiến trúc hệ điều hành Windows

- Windows dựa trên hạt nhân NT (đối với Windows NT, 2000, XP, 7, 8, 10, 11).
- Bao gồm các lớp: hạt nhân, giao diện người dùng, API hệ thống, hạ tầng bảo mật.

1.3.3 Giao diện Windows

- Giao diện đồ họa dựa trên cửa sổ, biểu tượng, thanh tác vụ.
- Bắt đầu từ Windows 95 với nút Start, Taskbar.
- Windows 8 giới thiệu giao diện Metro, Windows 10 và 11 kết hợp giao diện cụm ứng và cổ điển.

1.3.4 Đặc điểm đặc trưng của Windows

- Dễ dàng sử dụng, hỗ trợ đa dạng cụng và phần mềm.

- Tích hợp hệ sinh thái Microsoft, đồng bộ dữ liệu với OneDrive.
- Cập nhật bảo mật thường xuyên.
- Hỗ trợ cài đặt ứng dụng Android (Windows 11).

1.4 Phần mềm bảo vệ máy

1.4.1 Phần mềm diệt virus

Phần mềm diệt virus (Antivirus Software) là công cụ bảo vệ máy tính khỏi các loại virus gây hại bằng cách phát hiện, ngăn chặn và loại bỏ chúng khỏi hệ thống.

AVG AntiVirus là một phần mềm diệt virus phổ biến, cung cấp bảo vệ chống lại virus, phần mềm độc hại, ransomware và các mối đe dọa trực tuyến khác. Nó bao gồm các tính năng như quét thời gian thực, bảo vệ email, duyệt web an toàn và cập nhật cơ sở dữ liệu virus tự động. AVG AntiVirus có sẵn ở cả phiên bản miễn phí và trả phí, giúp người dùng bảo vệ thiết bị khỏi các nguy cơ bảo mật.

Các tính năng chính của AVG Antivirus bao gồm:

- Chống virus và phần mềm độc hại: Quét và loại bỏ virus, trojan, phần mềm gián điệp, và các phần mềm độc hại khác trên máy tính.
- Bảo vệ web: Phát hiện và ngăn chặn các mối đe dọa từ trang web độc hại khi bạn duyệt web.
- Bảo vệ email: Kiểm tra các email đến và đi, giúp ngăn chặn virus và phần mềm độc hại được gửi qua email.
- Chống lừa đảo trực tuyến: Ngăn chặn các trang web giả mạo nhằm đánh cắp thông tin cá nhân của bạn (như thông tin tài khoản ngân hàng hoặc thẻ tín dụng).

1.4.2 Phần mềm chống phần mềm gián điệp

Phần mềm chống phần mềm gián điệp (Anti-Spyware Software) bảo vệ hệ thống khỏi các chương trình theo dõi trái phép như keylogger, adware, rootkit.

Spybot S&D (Spybot – Search & Destroy) là một phần mềm bảo mật được sử dụng để phát hiện và loại bỏ phần mềm gián điệp (spyware), phần mềm quảng cáo (adware) và các loại phần mềm độc hại khác trên máy tính. Nó cung cấp các công cụ quét và diệt phần mềm độc hại, giúp người dùng bảo vệ sự riêng tư và an toàn của dữ liệu cá nhân khi duyệt web.

Spybot S&D có các tính năng như:

- Quét và loại bỏ phần mềm gián điệp: Phát hiện và xóa các phần mềm theo dõi hành vi người dùng mà không được phép.
- Chống phần mềm quảng cáo: Loại bỏ các chương trình quảng cáo gây phiền toái hoặc làm giảm hiệu suất máy tính.

- Công cụ tự động cập nhật: Đảm bảo rằng phần mềm luôn được cập nhật với các cơ sở dữ liệu mới nhất về phần mềm độc hại.

1.4.3 Phần mềm chống các phần mềm độc hại

Phần mềm chống phần mềm độc hại (malware) giúp bảo vệ máy tính và thiết bị khỏi các mối đe dọa như virus, trojan, ransomware, spyware, adware và các phần mềm gây hại khác

Malwarebytes Anti-Malware là một phần mềm bảo mật chuyên dụng, đặc biệt nổi bật trong việc xử lý các phần mềm độc hại mà các phần mềm diệt virus truyền thống có thể bỏ sót.

Các tính năng chính của Malwarebytes Anti-Malware bao gồm:

- Quét và loại bỏ phần mềm độc hại: Phát hiện và xóa bỏ virus, trojan, ransomware, spyware, adware, rootkit và các phần mềm độc hại khác.
- Chống ransomware: Phòng chống các cuộc tấn công mã hóa tống tiền, giúp bảo vệ các tệp quan trọng của người dùng.
- Quét nhanh và sâu: Malwarebytes cung cấp cả quét nhanh cho các khu vực có nguy cơ cao và quét sâu cho toàn bộ hệ thống để phát hiện mọi mối đe dọa tiềm ẩn.
- Chế độ khôi phục: Nếu máy tính bị nhiễm phần mềm độc hại nghiêm trọng, phần mềm có thể giúp phục hồi hệ thống và loại bỏ các mối đe dọa.
- Chống phần mềm gián điệp: Phát hiện và ngăn chặn phần mềm gián điệp thu thập thông tin cá nhân mà không có sự cho phép.
- Bảo vệ web: Tự động ngăn chặn các trang web độc hại khi người dùng duyệt web.

1.4.4 Phần mềm cứu hộ

Phần mềm cứu hộ giúp khôi phục hệ thống bị lỗi do virus, spyware hoặc sự cố phần cứng.

Kaspersky Rescue Disk (KRD) là một công cụ giúp người dùng loại bỏ virus và phần mềm độc hại mà không cần phải khởi động vào hệ điều hành chính của máy tính. Đây là một công cụ rất hữu ích khi máy tính bị nhiễm virus nặng hoặc không thể khởi động bình thường, vì nó chạy trực tiếp từ một đĩa CD, DVD hoặc USB bootable.

Các tính năng của Kaspersky Rescue Disk (KRD):

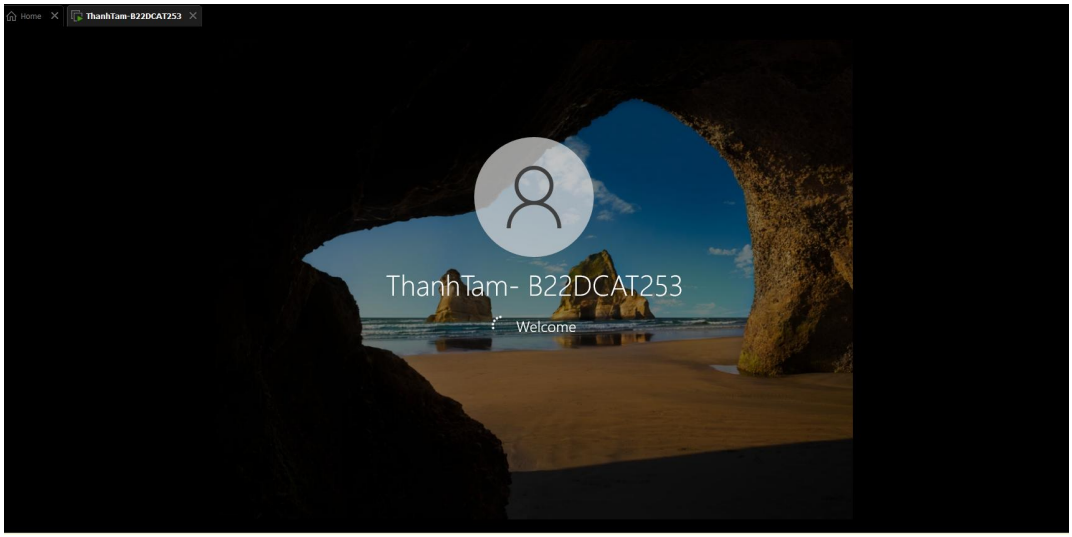
- Quét và loại bỏ virus: Phát hiện và loại bỏ virus, trojan, phần mềm độc hại.
- Chạy từ môi trường ngoài hệ điều hành: Hoạt động mà không cần khởi động Windows.
- Cập nhật cơ sở dữ liệu virus: Tải và cập nhật các mẫu virus mới nhất.
- Sửa chữa hệ thống: Khôi phục tệp hệ thống bị hỏng do virus.
- Giao diện dễ sử dụng: Thao tác đơn giản và dễ hiểu.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- File cài đặt Windows 10 định dạng iso.
- Phần mềm ảo hóa: VMWare Workstation.

Đặt tên máy là : "ThanhTam- B22DCAT253"



Hình 2 – Khởi động máy trạm

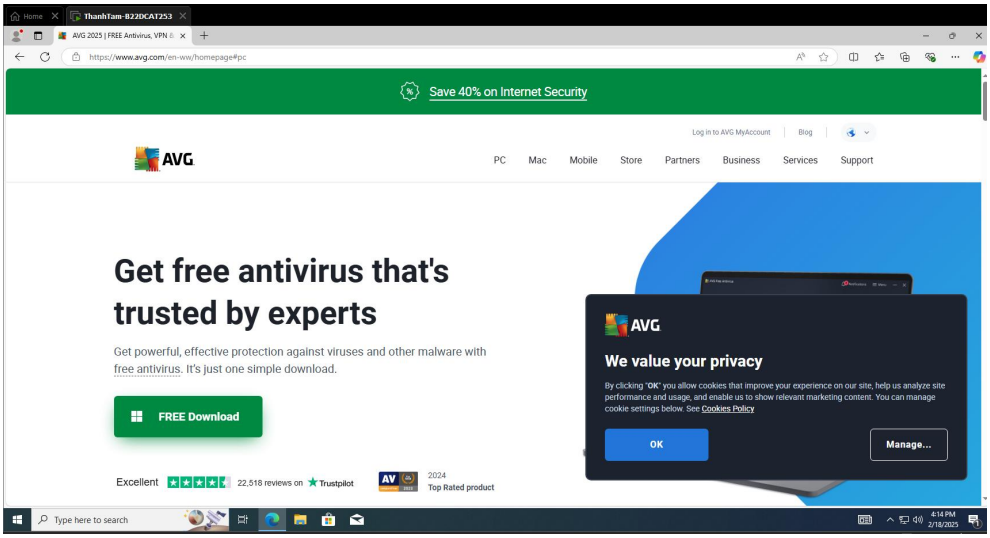
2.2 Các bước thực hiện

Thực hiện cài đặt và chạy một số phần mềm bảo vệ máy trạm sau:

2.2.1 Cài đặt phần mềm diệt virus: AVG AntiVirus

Bước 1: Tải phần mềm

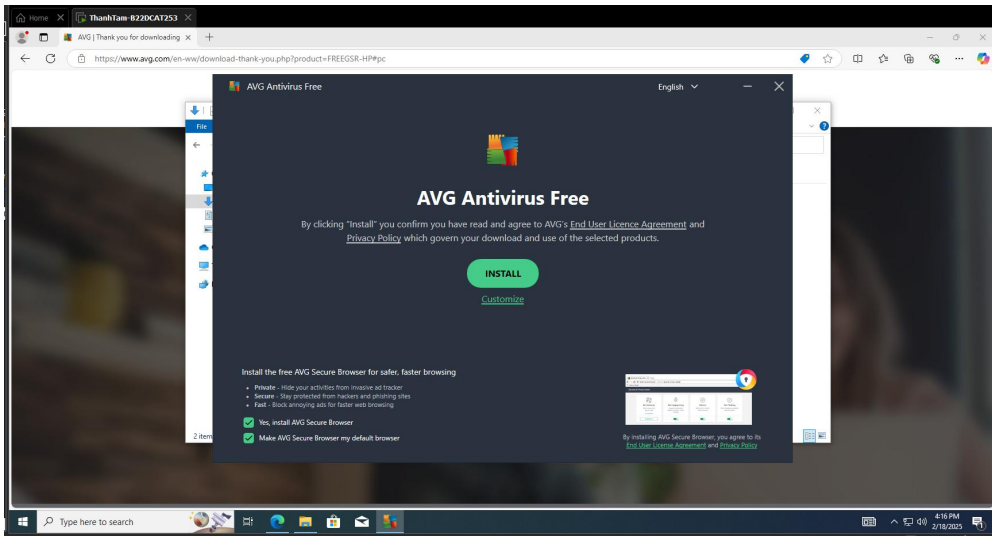
- Truy cập trang chính thức của AVG: http://www.avg.com
- Nhấn Free Download để tải miễn phí



Hình 3 – Trang chính thức của AVG

Bước 2: Cài đặt AVG AntiVirus

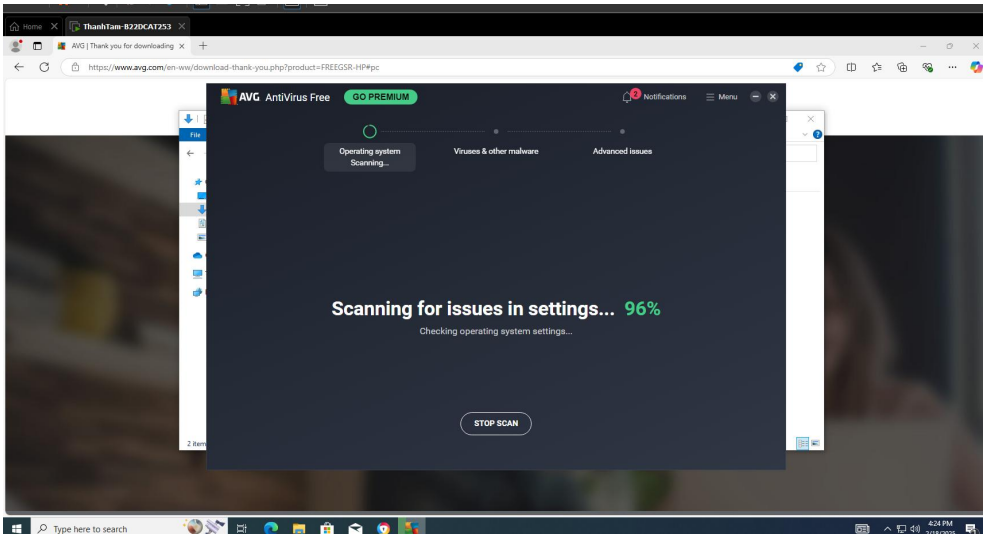
- Mởi file .exe vừa tải về -> Nhấn Install -> chờ cài đặt hoàn tất -> Nhấn finish



Hình 4 – Cài đặt AVG

Bước 3: Chạy thử và sử dụng phần mềm

- Nhấn Scan Computer để quét toàn bộ hệ thống

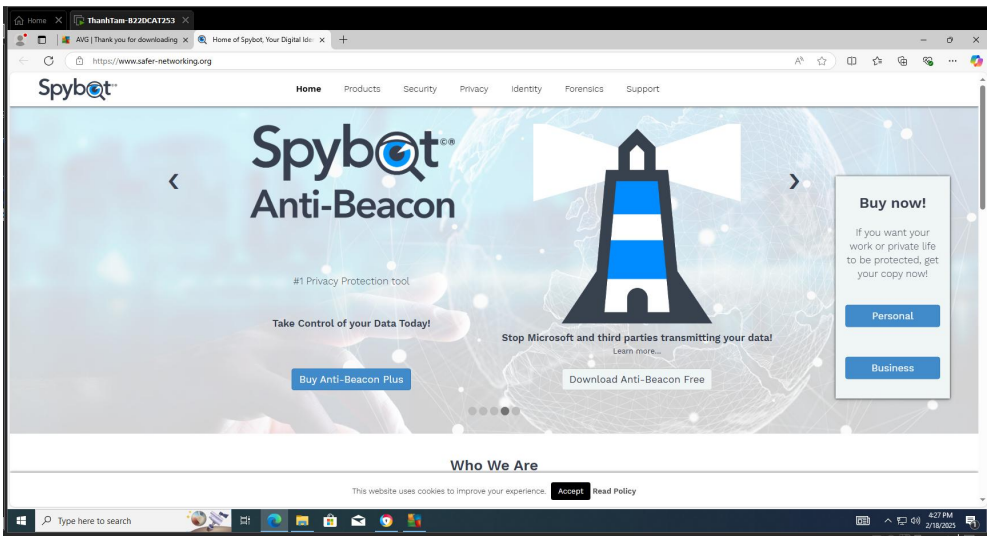


Hình 5 – Quét hệ thống bằng AVG

2.2.2 Cài đặt phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)

Bước 1: Tải phần mềm

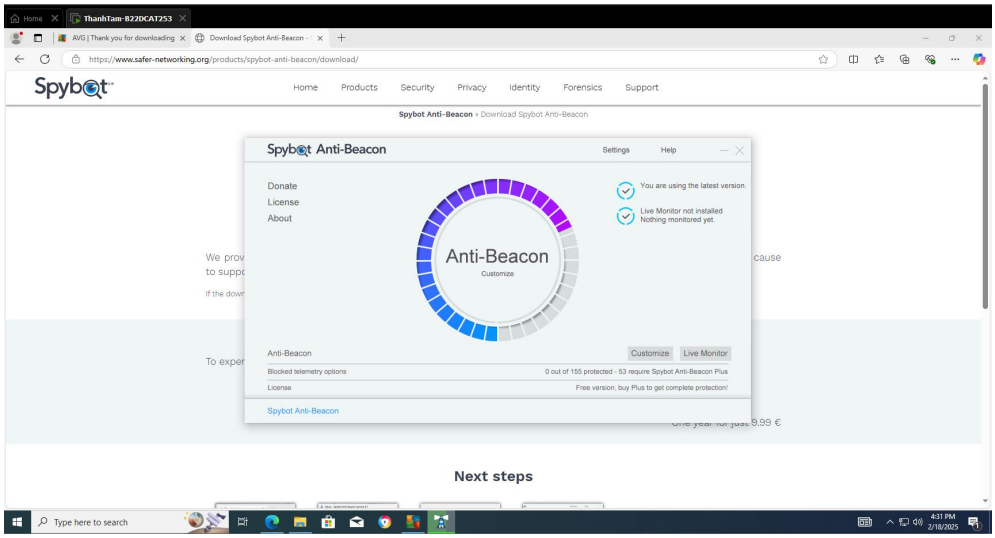
- Truy cập: http://www.safer-networking.org
- Chọn Dowload Spybot Free Edition.



Hình 6 – Trang chính thức của Spybot S & D

Bước 2: Cài đặt Spybot

- Mởi file .exe vừa tải về
- Chọn next và đồng ý điều khoản sủ dụng
- Nhấn Install và chờ quá trình cài đặt hoàn tất -> nhấn Finish



Hình 7 – Cài đặt Spybot S & D

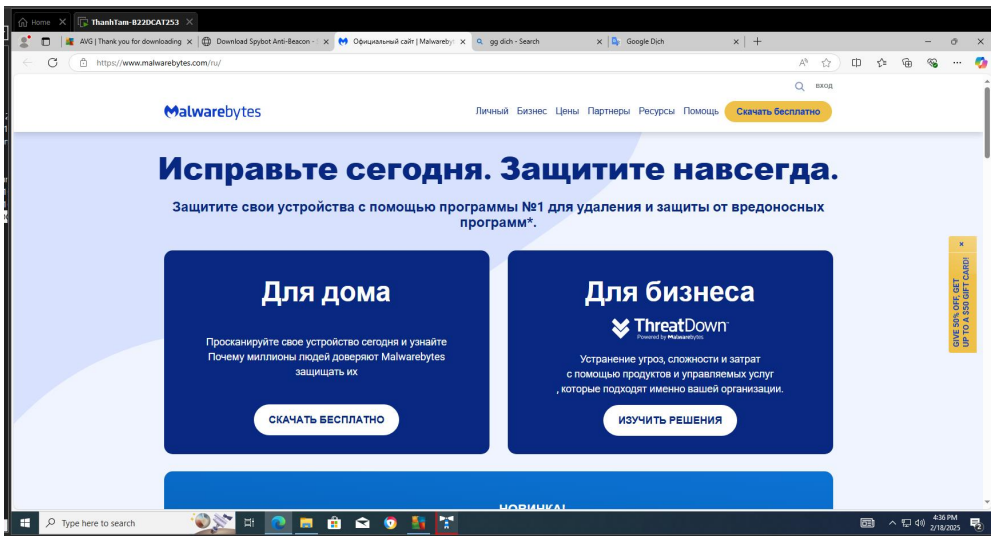
Bước 3: Chạy thử và sử dụng phần mềm

- Nhấn Scan để quét phần mềm gián điệp

2.2.3 Cài đặt phần mềm chống mã độc: Malwarebytes Anti-Malware

Bước 1: Tải phần mềm

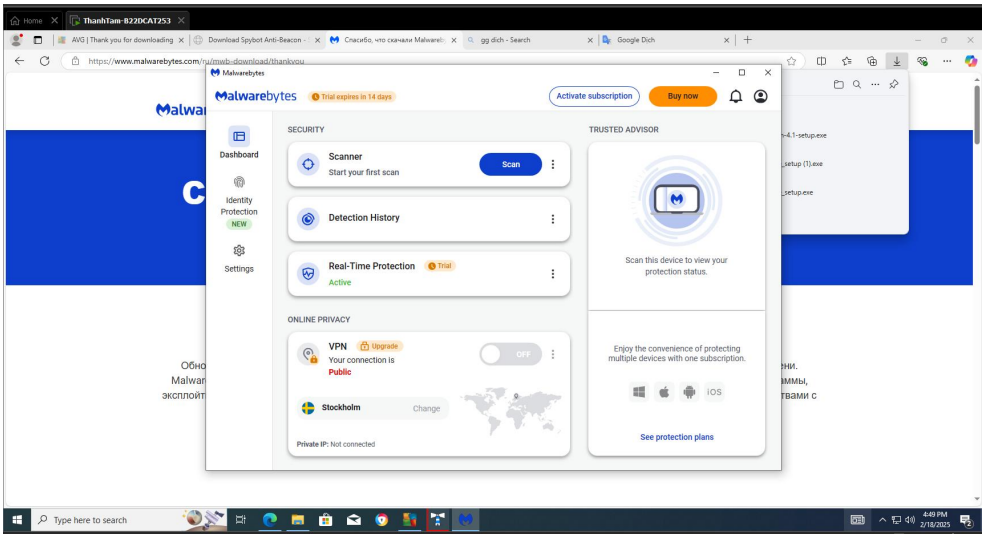
- Truy cập: http://www.malwarebytes.com
- Chọn Free Download



Hình 8 – Trang chính thức của Malwarebytes Anti-Malware

Bước 2: Cài đặt Malwarebytes

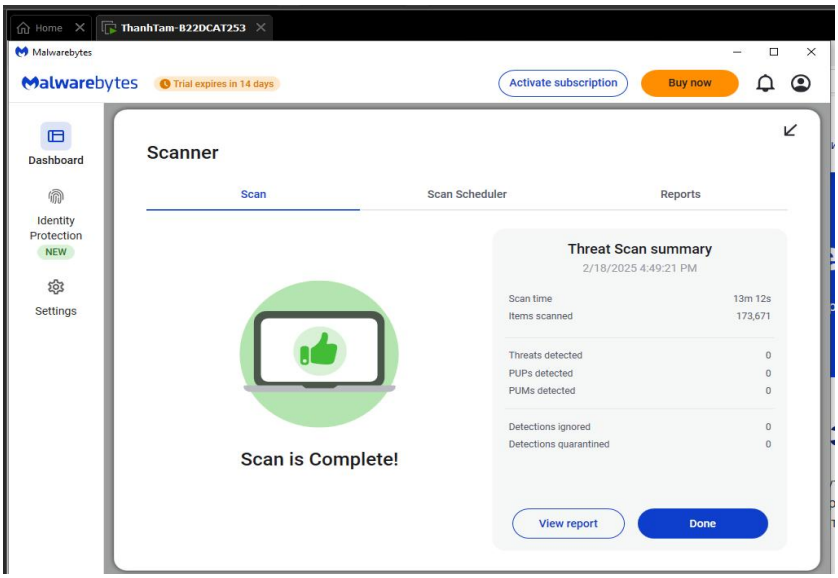
- Mởi file .exe vừa tải về
- Chọn Personal Computer và nhấn next
- Nhấn Install và chờ quá trình cài đặt hoàn tất -> nhấn Finish



Hình 9 – Cài đặt Malwarebytes Anti-Malware

Bước 3: Chạy thử và sử dụng phần mềm

- Nhấn Scan



Hình 10 – Phần mềm hoàn tất quét

2.2.4 Cài đặt phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

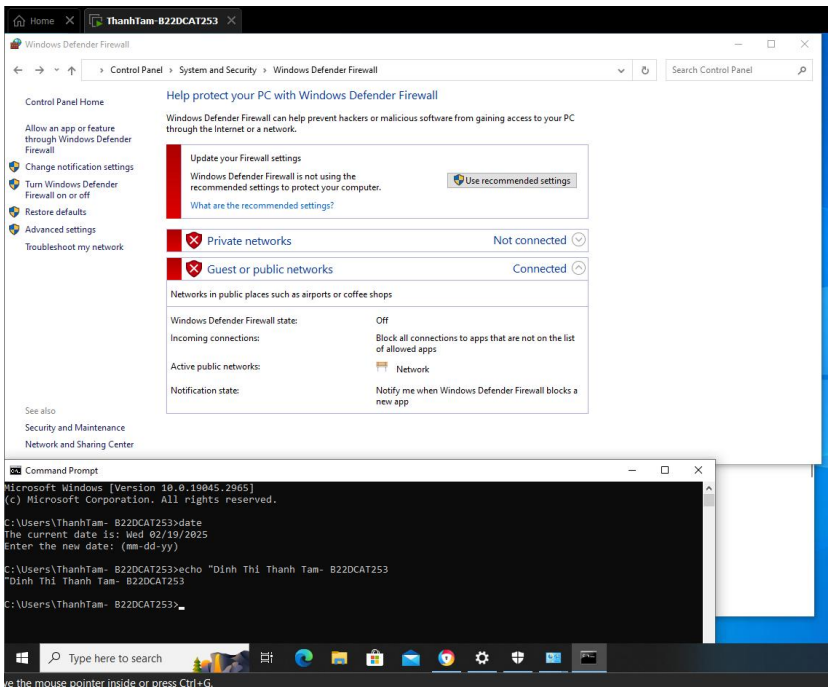
Bước 1: Tải file iso của Kaspersky Rescue Disk (KRD)

- https://www.kaspersky.com/downloads/free-rescue-disk
- Nhấn Dowload để tải file .iso

Bước 2: Tải file mã độc về máy trạm

- Dùng Web Browser tải file test mã độc từ đường link: http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe
- Lưu file test vào ổ C của máy trạm

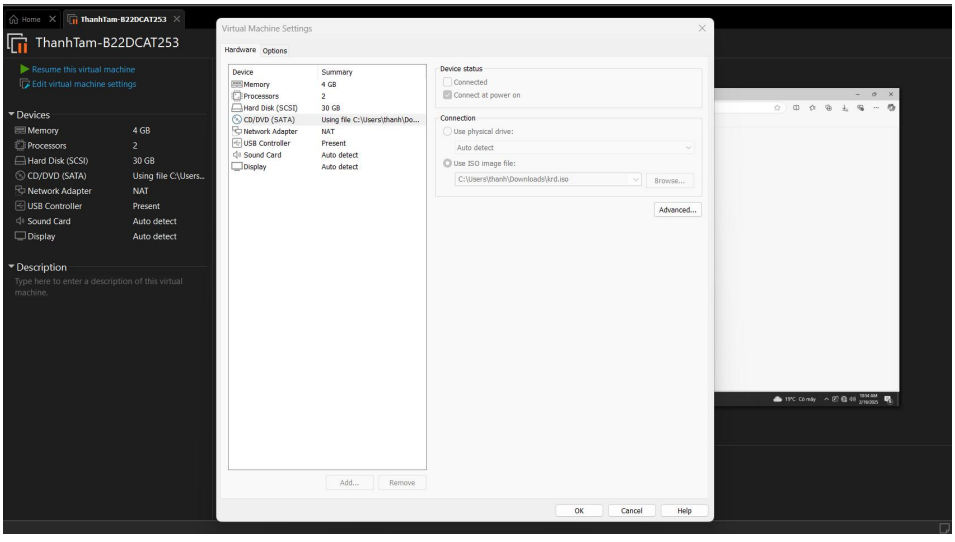
Note: trước khi tải file test nên tắt firewall và Windows security



Hình 11 – Tắt Firevall để tải file chứa mã độc không bị chặn

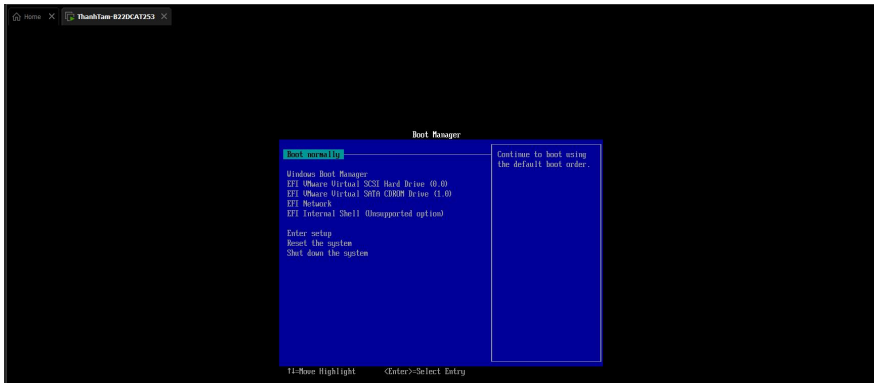
Bước 3: Load file iso vào máy ảo

- Mở Vmware Workstation
- Vào Setting -> CD/DVD (SATA) -> chọn Use ISO image file.
- Chọn file krd.iso vừa tải về



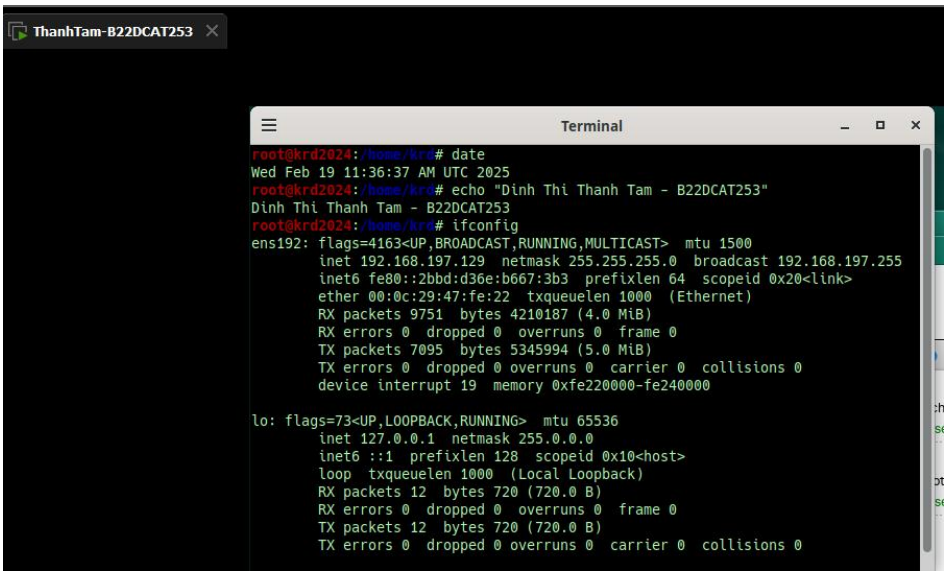
Hình 12 – Load file iso KRD vào máy ảo

- Khởi động lại máy ảo
- Khi máy ảo khởi động, nhấn ESC để mở Boot menu -> chọn boot từ CD-ROM drive để cài đặt KRD



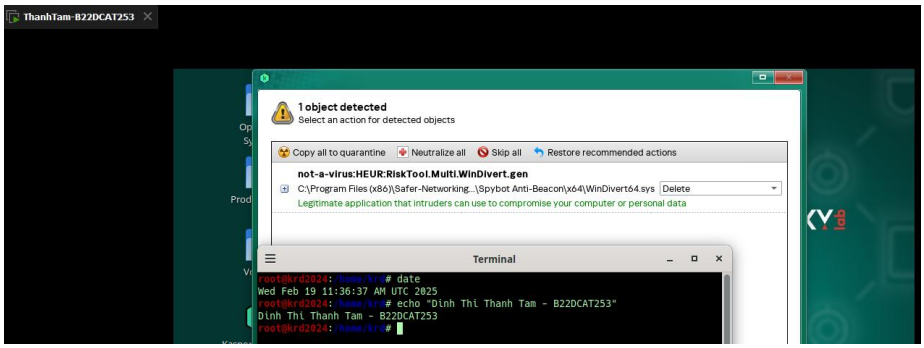
Hình 13 – Chọn boot từ CD-ROM drive

- Mở cmd kiểm tra IP của máy trạm bằng câu lệnh: ifconfig



Hình 14 – Kiểm tra IP của máy trạm

- Sau đó chạy Kaspersky Rescue Tool để quét tất cả các thư mục và phát thiện ra file test



Hình 15 – Quét thành công file chứa mã độc

- Đã tìm được file test chứa mã độc, chọn delete -> continue để loại bỏ file

KẾT LUẬN

- Cài đặt thành công Windows 10
- Cài đặt và chạy thành công các phần mềm bảo vệ máy trạm theo yêu cầu

TÀI LIỆU THAM KHẢO

[1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.

[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.